Übungen zur Vorlesung
Entscheidungsverfahren mit
Anwendungen in der Softwareverifikation

Wintersemester 2019/20

Aufgabenblatt 2

Institut für Theoretische Informatik, Karlsruher Institut für Technologie (KIT) 18.11.2019

Prof. Dr. Carsten Sinz Abgabe: 02.12.2019

Aufgabe 4 (lineare diophantische Gleichungssysteme) [10(+10) Punkte]

Implementieren Sie das Verfahren zur Lösung von linearen diophantischen Gleichungen aus der Vorlesung in einer Programmiersprache Ihrer Wahl.

Die Eingabe Ihres Programms ist ein Gleichungssystem bestehend aus m Gleichungen der Form $a_1x_1 + \cdots + a_nx_n = b$, das in einer Datei mit folgendem Format abgelegt ist:

1. Die erste Zeile besteht aus zwei Zahlen, m und n, die für die Anzahl der Gleichungen (m) und die Anzahl der Variablen (n) stehen.
2. Darauf folgt in jeder Zeile die Repräsentation einer Gleichung, die wie folgt dargestellt ist:
   (a) Die erste Zahl, t, ist die Anzahl der Terme in der Gleichung (d.h. der x_i mit Koeffizienten ungleich 0 plus eins für die Konstante auf der rechten Seite der Gleichung).
   (b) Darauf folgen $(t-1)$-mal zwei Zahlen, c und i, die jeweils für einen Term $c \cdot x_i$ stehen. Die Indizes i sind dabei in aufsteigender Reihenfolge sortiert.
   (c) Darauf folgt eine Zahl, die für die rechte Seite der Gleichung, also b, steht, gefolgt von einer abschließenden 0.

Das Gleichungssystem

$$\begin{aligned} 2x_1 + 3x_3 - 4x_5 &= 10 \\ -x_1 - 7x_2 + 3x_4 + x_5 &= -5 \\ x_2 + x_3 &= 1 \end{aligned}$$

wäre also durch die folgende Datei beschrieben:

```
3 5
4 2 1 3 3 -4 5 10 0
5 -1 1 -7 2 3 4 1 5 -5 0
3 1 2 1 3 1 0
```

Die Ausgabe Ihres Programms soll aus einer Zeile bestehen, die entweder den Text `SAT` oder `UNSAT` enthält, je nachdem, ob das Gleichungssystem über den ganzen Zahlen lösbar ist oder nicht. In ersterem Fall soll darauf eine Zeile folgen, die die Lösung angibt. Diese soll aus n Zahlen bestehen, wobei die i-te Zahl für den Wert x_i der Lösung steht.

Unter `https://baldur.iti.kit.edu/EAS/lin-eq-ex.zip` können Sie Testdaten für Ihr Programm herunterladen. Für ein korrektes Programm gibt es 10 Punkte, für die drei besten Programme zusätzlich bis zu 10 Bonuspunkte (10 für das schnellste, 8 für das zweitschnellste und 5 für das drittschnellste).

Aufgabe 5 (SAT als lineares Ungleichungssystem) [4 Punkte]

Geben Sie an, wie ein aussagenlogisches Erfüllbarkeitsproblem (in konjunktiver Normalform) als lineares Ungleichungssystem über den ganzen Zahlen (d.h. in der Logik LIA) codiert werden kann. Was folgt daraus für die Komplexität eines Entscheidungsverfahrens für die Logik LIA?

Aufgabe 6 (SAT mit beschränktem Variablenvorkommen) [3 Punkte]

Zeigen Sie: Das SAT-Problem, eingeschränkt auf Formeln, in denen jede Variable maximal 3-mal vorkommt, ist bereits NP-vollständig. Geben Sie dazu eine Transformation an, die eine beliebige aussagenlogische Formel in konjunktiver Normalform in eine erfüllbarkeitsäquivalente Formel transformiert, in der jede Variable höchstens 3-mal vorkommt.

Aufgabe 7 (lineare diophantische Gleichungssysteme) [3 Punkte]

Im in der Vorlesung betrachteten Verfahren zur Lösung ganzzahliger linearer Gleichungssysteme wird im Substitutionsschritt die Umformung von

$$-a_k m\sigma + \sum_{i\neq k}(a_i + a_k(a_i \bmod' m))\cdot x_i = c + a_k(c \bmod' m)$$

nach

$$-a_k\sigma + \sum_{i\neq k}(\lfloor a_i/m + \frac{1}{2}\rfloor + (a_i \bmod' m))\cdot x_i = \lfloor c/m + \frac{1}{2}\rfloor + (c \bmod' m)$$

vorgenommen. Weisen Sie nach, dass diese Umformung korrekt ist.